



Customs-Trade Partnership Against Terrorism Alert

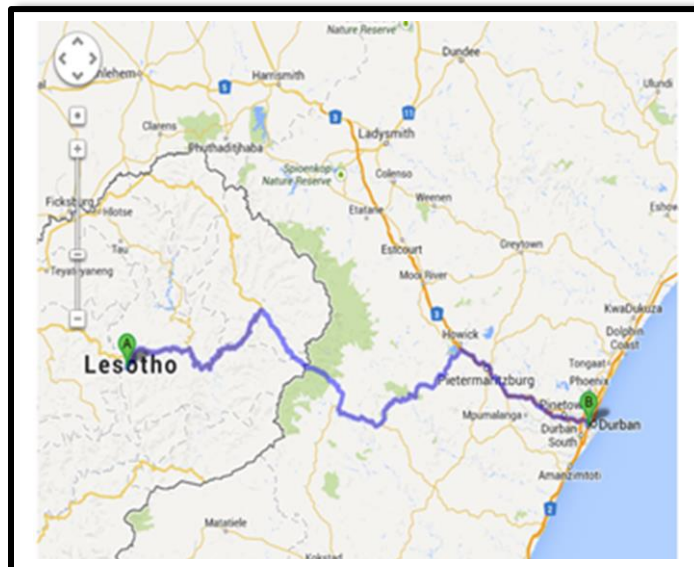
South Africa – Risk of Pilferage/Cargo Manipulation

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP has successfully worked with the trade community to strengthen international supply chains and improve U.S. border security. An integral part of this partnership entails CBP's and the trade community's willingness to share information about potential threats to, and security breaches within, international supply chains.

To enhance communication with its members, C-TPAT routinely highlights security matters for the purpose of raising awareness and renewing Partners' vigilance regarding supply chain security.

This notice alerts C-TPAT importer Partners sourcing from South Africa to an identified trend. CBP has confirmed several instances of containerized cargo pilferage and/or manipulation between Lesotho and the Port of Durban, South Africa. This route is approximately 282 miles long and takes about 8 hours to cover. Wearing apparel and textile importers have been particularly hit by thieves who steal the original cargo while in transit and then counterbalance the container with items of no value so that the weight of the container remains the same as the original weight so as not to alert local Customs officials. It is not unusual to find employees of local companies involved in cargo theft in South Africa.

According to Freight Watch International's *2013 Global Cargo Theft Threat Assessment*, "violent cargo crime — truck hijackings and facility robberies — remained a common and widespread issue in South Africa in 2012. This is the case even though the latest crime statistics from the South African Police Service (SAPS) show a 17.8% decrease in the number of truck hijackings between April 2011 and March 2012. According to these figures, 821 trucks were hijacked over the 12-month period as compared with 999 during the same period a year earlier."



Trade Route Between Lesotho and the Port of Durban, South Africa



Recommendations

C-TPAT highly recommends that importers re-assess supply chain risk factors facing containerized shipments routed through the southern region of the African continent. Importers are advised to review their regional supply chains against the following C-TPAT Minimum Security Criteria:

Risk Assessment - Provide direct outreach to vendors and service providers in the affected region regarding the importance of security measures.

Communicate C-TPAT criteria regarding seal control, container tracking and monitoring, and procedural security to local business partners.

Conveyance Tracking and Monitoring Procedures - If GPS is in place, ensure that it is being utilized as a live monitoring tool – not simply as a record to be referenced at a later date.

Encourage the use of geo-fencing technology to generate alerts when a conveyance strays from a predetermined route.

Maintain constant communication with the driver, tractor and trailer while en route to the seaport. Implement designated times/locations at which drivers are to report to dispatch.

Procedural Security - Ensure that local factory managers, freight forwarding personnel, and transportation providers understand procedures on reporting suspicious activities, weight discrepancies, and/or other anomalies.

Importers should work with foreign vendors and service providers to confirm clearly established protocols for reporting pilferage, weight discrepancies, and other security breaches.

C-TPAT partners are required to have firmly established response and reporting procedures *throughout* their respective supply chain(s). Importers should ensure that reporting procedures are in place to stop a suspicious shipment from leaving Africa. Failing that, importers should establish procedures allowing a suspicious shipment to be reported at the earliest possible time thereafter.

Security Threat and Awareness Training - Importers should request that vendors and supply chain service providers conduct refresher training on supply chain security topics.

Training should be provided to employees handling cargo and especially truck drivers on topics such as detecting internal conspiracies, container seal control, reporting weight discrepancies, and container tracking.



Highway Carrier Environment – Best Practices

Members have developed several Best Practices (refer to the C-TPAT Best Practice Catalog for additional information) to defeat security breaches. Some of these best practices include:

- Designated time spots – driver must report time at each specific area along the route.
- Minimize/eliminate un-necessary stops by drivers throughout the transportation route. All stops must be made at approved locations.
- Highway Carrier company has the ability to remotely shut off the truck's engine in the event of route deviations / lost contact with driver.
- Use of tamper-indicative security labels bearing an actual photo of the seal and a serial number, attached to the hinges and between the two doors of the vehicle.
- Use of multiple ISO/PAS 17712 certified high security seals on all shipments bound to the U.S.
- For company owned trailers – utilize spot welded bolts and other hardware (such as hinge covers) to avoid tampering.
- In addition to using a bolt seal, attach a cast iron J-bar device to the locking bar that requires a specialized tool for removal.
- Shipping documents are held at the last checkpoint and crossing documents provided only if shipment arrived within prescribed timeline and original high security seal is intact. Shipments not meeting timelines are ordered back to plant for formal investigation and inspection or an alert should be sent to the appropriate government authorities.
- Implement substantial internal controls and regular audits to oversee transportation providers and the conveyance monitoring processes.
- The importer established an internal global supply chain security team responsible for assessing risk within the company's international supply chains. The team exercises complete control and oversight of all security related matters, ensures that corporate standards are applied uniformly throughout all company facilities and verifies compliance with these security standards via onsite audits.



U.S. Customs and
Border Protection

How to Alert CBP

C-TPAT requires and encourages Partner notification of suspicious activities, anomalies, and security breaches.

1. Contact CBP personnel in Durban, South Africa, who work under CBP's Container Security Initiative or CSI.

CBP Officer Kendra Holloway – kendra.holloway@cbp.dhs.gov

CBP Officer Robert Fehr – robert.fehr@cbp.dhs.gov

2. Contact your port of entry. To find your local CBP port of entry's telephone number, please navigate to the site below:

<http://www.cbp.gov/xp/cgov/toolbox/ports/>

3. Call the CBP hotline 1-800-BE ALERT (1-800-232-5378)

**Re-Assess Risks
Mitigate Vulnerabilities
Apply Best Practices
Report Suspicious Activities**

C-TPAT Appreciates Your Continued Effort to Secure the International Supply Chain.

C-TPAT Program

Cbp.gov/ctpat
1300 Pennsylvania Avenue, NW
Washington, DC 20229

(202) 344-1180

Industry.partnership@dhs.gov



U.S. Customs and
Border Protection